CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

The CyberPeace Institute's Statement at the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

Madame Chair, Distinguished Delegates,

The CyberPeace Institute appreciates the opportunity provided to the representatives of the multistakeholder community to participate in the discussions of the Ad Hoc Committee.

The negotiations take place at a time of rapid changes in the rate, scale, and diversity of cybercrimes. Malicious actors increasingly target critical infrastructure and vital services with negative impacts and harm to people. The damage wrought by cybercrime has an important human component. For example, when a cyberattack targets the healthcare or the humanitarian sector, the impact on the safety and well-being of people is stark.

Drafting a cybercrime treaty must be a collective effort. Civil society can contribute by providing knowledge of how potential threats impact human rights and by building research and experience-based understanding informed by the proximity to victims of cybercrime.

For instance:

(1). The CyberPeace Institute has been facilitating the mapping and analysis of cyberattacks in the healthcare sector and the humanitarian sector and in times of conflict.

(2). The Institute has been also working closely with the most vulnerable victims of cyberattacks. Under the CyberPeace Builders program, it coordinates recovery efforts after cyberattacks and helps humanitarian NGOs become more cyber resilient.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

These and many other positive examples from the multistakeholder community illustrate the value of diverse stakeholders' contributions, and we welcome the opportunity to provide comments on the Consolidated negotiating document.

We listened carefully to the interventions, and we would like to raise five points for consideration based on our expertise.

(1.) We recommend that the convention keeps the scope of application on cyber-dependent crimes that require ICT infrastructure for them to be committed. A focus on serious criminal offences will contribute to streamlining processes and procedures covered in the convention and allowing for effective implementation of the treaty.

(2.) The convention needs to incorporate robust human rights safeguards to ensure independent oversight and effective redress mechanisms. An effective criminal justice system that prevents and counters criminal activities must be rooted in the protection and promotion of human rights. The convention should emphasize the role of international human rights law, and mainstream human rights protections across the document.

(3.) The convention should focus on victim protection. Cyberattacks against critical services and organizations affect vulnerable people both physically and online. States should consider different kinds of harm inflicted by cyberattacks and connected issues of re-victimization and redress. This is particularly important in cases affecting vulnerable groups, or people in vulnerable situations, such as those impacted by cyberattacks targeting the healthcare sector and humanitarian organizations.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
https://cyberpeaceinstitute.org

(4.) The convention should require a standard of clear criminal intent. It must be ensured that legitimate activities of cybersecurity researchers, technology companies, and others for activities that are essential to overall cyber security and cyber resilience are not threatened by criminalization.

Last, but not least – as Article 42 has been discussed, the Institute would like to highlight that the convention should:

(5.) Define the government access to data narrowly and precisely to meet specific needs for public safety and national security. The provisions on procedural matters and law enforcement must follow the principles of proportionality, necessity, and legality, and be accompanied with mechanisms safeguarding human rights and protections against possible misuse.

Finally, the Institute believes that the inclusiveness of the Ad Hoc Committee should serve as an inspiration and positive precedent for other cyber-related discussions at the United Nations and elsewhere – and we look forward to engaging in forthcoming sessions.